EUROSMART
The Voice of the Digital Security Industry

How to ensure that identity services in Europe are preserving Europe's sovereignty?

Context

The European Commission will soon present a proposal for a European Digital Identity (EUid). Different options are currently envisaged. One of these options is to create a new trust service, pursuant to the eIDAS Regulation, for (private) electronic (or digital) identity providers. This paper highlights the position of Eurosmart on this topic. Eurosmart sees many potential pitfalls in this approach that should be carefully assessed by policymakers. Eurosmart drew recommendations to prevent these pitfalls.

Eurosmart's position: digital sovereignty as a guiding principle

On 28 October 2020, the CEOs of technology giants Facebook, Google and Twitter testified during a US Senate hearing on the topic of tech companies' treatment of hate speech and misinformation on their platforms.[1] This hearing took place in a context of growing concerns regarding the negative impacts of big tech. Many news tells the story of **social accounts suspended "by error"**. These stories might become a nightmare when this account is your EU identity.

In the future framework of an EU universal digital identity, where private companies are trusted identity services providers, **EU policymakers must avoid the situation where CEOs can decide who has access to digital services and who has not**. EU policymakers will have a vital responsibility to offer digital identity services to all European citizens and **keep it under the control of national states and EU jurisdiction**.

Eurosmart would like to highlight the following points to ensure that digital sovereignty and security are at the heart of this future EU digital identity project.

Digital identity providers are too important to be ruled like any other trust services

As a starting point, it is important to underline that **providing digital identity is not a mere trust service, it is the foundation of all trust services.** For this reason, additional requirements should apply to digital identity providers, beyond those that already apply to trust service providers.

On top of the eIDAS security requirements, digital **identity providers must be regulated according to EU values**. Special regulation for digital identity providers must enforce obligations stemming from their particular roles.

[1] Marcy Gordon, "CEOs of 3 tech giants to testify at Oct. 28 Senate hearing", ABC News, 5 October 2020.

Moreover, governance transparency must be mandatory to ensure that citizen's digital identity is not under the influence of non-European entities or interests, nor is affected by organised criminal networks.

Policymakers must also ensure that a comprehensive screening, risk management assessment and clearance ("Know-your-identity-provider" risk management assessment) is carried out before delivering agreement to digital identity providers.

More precisely digital identity providers must comply with the following key principles:

- **Digital identity providers must offer to EU citizens universal and equal access to online services**, regardless of a person's nationality, gender, language group, political position, culture, profession, disability or sexuality. AI algorithms – if used - must be not discriminatory;
- **Digital identity providers must not alter citizen's attributes or national root identity**;
- **The digital identity system must be interoperable by design**, so that citizens are able to transfer identity and identity attributes between digital identity providers;
- **Digital identity cannot be asserted without express consent of its holder**;
- **Privacy and security must be guaranteed by design**;
- **The digital identity cannot be separated from its holder**. It shall not be possible for anyone to lose its digital identity, or have it stolen in a way where it cannot be recovered, leading to divest the legitimate holder of its digital identity;
- **If a device holding the digital identity credential is lost, the holder shall be able to revoke it**;
- **Should the holder lose control of his/her account** (i.e. following a hacking performed by an attacker), **there must be a way for the legitimate holder to recover his identity**.

Introduce a requirement of Europeanity

Eurosmart believes that Europeanity is a further requirement that deserves full attention from policymakers. Digital identity is an enabler to access the digital world, and thus for the Digital Single Market (DSM). Therefore, in order to ensure that national and European laws are enforced in the digital world, it is key to ensure that digital identity providers are effectively ruled by these laws and courts.

⇨ As a matter of fact, a mechanism shall be put in place to ensure that a digital identity provider, falling under the provisions of the future legislative instrument to come, is effectively governed by national and European laws to ensure national and European laws will be effectively applied. This mechanism should rely on a criterion of Europeanity, which does not exist as such for trust services.

⇨ More precisely, Eurosmart suggests the adoption of the following requirements for identity providers:

- Digital identity providers must be European registered companies or European public entities;
- Digital identity providers' Ultimate Beneficial Ownerships (UBO) must be European citizens.

Establish sovereign control over the types of entities able to provide eID

While it is not explicitly said, many Member States fear that GAFAM take advantages of this approach to be recognised as digital identity providers within EEA falling under the provisions of the future legislative instrument to come. This possibility is not acceptable for some of them as it could cause (1) a loss of sovereignty over transaction in the digital world, and (2) a foreclosure effect for any other European actors, leading to kill the emergence of European alternatives and ecosystem.

- ⇨ Therefore, a mechanism shall be put in place to ensure a kind sovereign control over the type of entity that could be a digital identity provider falling under the provisions of the future legislative instrument to come.

Legislate on security for identification and authentication means

The current implementation of (qualified) trust services under eIDAS regulation has opened the door to server signing (remote identification and authentication). There are no clear security requirements or criteria in the eIDAS Regulation -and the corresponding Implementing Acts- to ensure the security of the local component (with which the holder interacts) performing the remote identification and authentication of the signatory. The legislation only lays down security requirement for the remote server performing the signature, but does not address at all the local components (with which the holder interacts) performing the remote identification and authentication of the signatory.

The creation of a (qualified) trust service for digital identity provider shall not lead to such situation where the remote identification and authentication of a holder towards a remote proxy – performing the authentication on behalf on the holder - is not covered by any sound, precise and well-defined security requirements. For digital identity providers, the basis for security and trust lies in the local components (with which the holder interacts). This local component shall be covered by clear and non-ambiguous security requirements covering both identification AND authentication of the holder.

- ⇨ The regime to be applied to digital identity providers shall be much more stringent than the one applied to trust service providers. The legal regime applied to a trust service provider under eIDAS considers that it is liable by default and manages its risk, it can freely put in place any measures it considers relevant to identify and authenticate the signatory.

  Eurosmart considers that in the case of digital identity provision, this approach is not sufficient. Should a security flaw exist in the way the holder is identified or authenticated, the risk management provided by the identity provider may not be sufficient. Even if the digital identity provider is held liable, the holder may also be held directly liable in some cases, for instance relevant to penal law. In that regard, the means of identification and authentication of the holder shall also be ruled by the legislator and shall not only rely on a risk management performed by the digital identity provider.

Take advantage of the Cybersecurity Act certification framework

As stated in the impact assessment, ever-increasing number of digital ID solutions are being developed. All answer different needs from public services, or private sector such as banking or social networks. To ensure a trustworthy development of the Digital Single Market, the certification of digital identity scheme at the adequate security level is of utmost importance, as it is the trust anchor to access any IT infrastructure. A cybersecurity breach on a digital identity scheme could lead to major damages both on citizens but also on critical infrastructure themselves. Such major risks shall be countered through mandatory security certification imposed on digital identity schemes, whether they are deployed under the eIDAS regulation or the future framework for private actors.

- ⇨ Eurosmart calls on the European Commission to rely on the Cybersecurity Act when it comes to security certification of digital identity schemes. An alignment between the eIDAS Levels Of Assurance (LoA) and the Cybersecurity Act would solve the issue of fragmentation, hence simplifying certification for companies, and would also clearly demonstrate the security of digital identity schemes. eIDAS LoAs should follow or refer to the three levels of the Cybersecurity Act (High, Substantial, Basic) in order to give consistency to certification in Europe.

Conclusion

Eurosmart recommends the European Commission not to create another trust service covering digital identity provision. By contrast, Eurosmart calls on the Commission to consider another regime for (private) digital identity providers. This regime would be different from the one applying to (qualified) trust services -as defined by eIDAS. This would preserve eIDAS certified sovereign IDs while private digital identities could still prosper in their own legal framework.[2] This regime shall be specific to (private) digital identity providers and shall take into account the elements aforementioned.

[2] Eurosmart, "Feedback on an EU Digital Identity scheme (EUid)", September 2020.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **GS TAG**, **Huawei**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **Sarapis**, **SGS**, **STMicroelectronics**, **Thales**, **Tiempo Secure, Toshiba**, **Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**,), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 36 35 | mail Contact@eurosmart.com